CISCO SYSTEMS

Getting Started Guide

Cisco Catalyst Blade Switch 3020 for HP Getting Started Guide

INCLUDING LICENSE AND WARRANTY

1 Introduction

2 Taking Out What You Need

3 HP c-Class BladeSystem Architecture

4 Installing the Switch Module in the Blade Server

5 Running Express Setup

6 Managing the Switch Module

7 In Case of Difficulty

8 Obtaining Documentation

9 Documentation Feedback

10 Cisco Product Security Overview

11 Obtaining Technical Assistance

12 Obtaining Additional Publications and Information

13 Hardware Warranty Terms

1 Introduction

This guide provides instructions on how to install your Cisco Catalyst Blade Switch 3020 for HP—hereafter referred to as the *switch module*—in the HP c-Class BladeSystem and to set up and configure your switch module. The HP c-Class BladeSystem—hereafter referred to as the *blade server*—supports up to eight Ethernet switch modules, which are installed in the interconnect bays of the blade server.

This guide also covers management options and troubleshooting help for the switch module.

For details on the numbers, types, and the location of the blade server bays, for additional information on the blade server system, and for detailed port mapping information, see the HP BladeSystem enclosure installation poster or the HP BladeSystem enclosure setup and installation guide at http://www.hp.com/go/bladesystem/documentation.

For additional installation and configuration information about the switch module, see the Cisco Catalyst Blade Switch 3020 for HP documentation on Cisco.com. For system requirements, important notes, limitations, open and resolved caveats, and last-minute documentation updates about the switch module, see the release notes, also on Cisco.com.

When using the online publications, refer to the documents that match the Cisco IOS software version that is running on the switch module. See the "Obtaining Documentation" section on page 1-24 for more information about the switch module publications.

For translations of the warnings that appear in this publication and all safety and handling warnings for this product, see the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3020 for HP* that accompanies this guide.

Before proceeding, read the release notes for the blade server. The release notes are available on the HP support website at www.support.hp.com.

2 Taking Out What You Need

These items ship with your switch module:

- Console cable
- *Cisco Catalyst Blade Switch 3020 for HP Getting Started Guide* (this book)
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3020 for HP*
- Registration card

Follow these steps:

1. Unpack and remove the switch module and the accessory kit from the shipping box.
2. Return the packing material to the shipping container, and save it for future use.

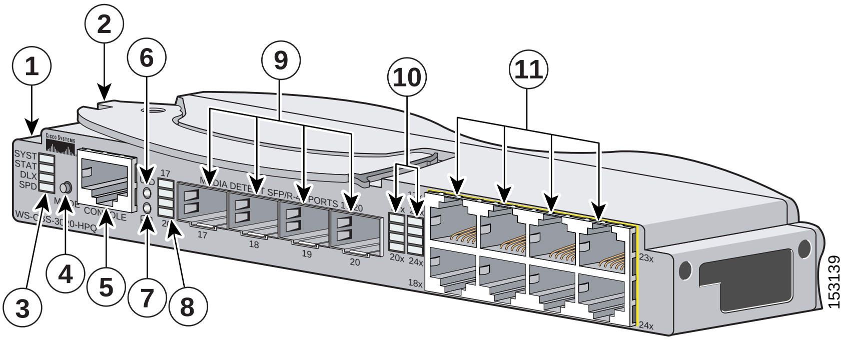
If the switch modules are ordered with the blade server, the switch modules are already installed. The unpacking procedure for the switch module applies only if one is ordered separately. See the blade server documentation for the unpacking procedure for the HP equipment.

Cisco Gigabit Ethernet Switch Module Description

The Cisco Catalyst Blade Switch 3020 for HP is a 24 Gigabit Ethernet port, Layer 2+ switch module. Sixteen of the Gigabit Ethernet ports are internal 1000BASE-X downlink ports that connect to the blade server. The other eight Gigabit Ethernet ports are external uplink ports that provide connections to other switches or routers. Uplink ports operate at 10/100/1000 Mbps if used as RJ-45 ports and operate at 1000 Mbps if small form-factor pluggable (SFP) fiber-optic modules are installed. See Table 1 for more detailed descriptions of the switch module ports.

Figure 1 shows the switch module.

Figure 1 The Catalyst Blade Switch 3020 for HP



1	Switch module	**7**	Health LED
2	Release latch	**8**	SFP module port LEDs for ports 17 to 20
3	System status LEDs	**9**	SFP module ports 17 to 20
4	Mode button	**10**	Gigabit Ethernet ports LEDs for ports 17x to 24x
5	Console port	**11**	Gigabit Ethernet ports 17x to 24x
6	UID[1] LED		

[1] UID: unit identifier

The switch module is managed through the RS-232 console port that uses an RJ-45 connector in the switch module front-panel.

The blade server includes a chassis management module, the Onboard Administrator. Each switch module connects internally to the Onboard Administrator through 100BASE-T Ethernet links. You can manage the switch modules through the Onboard Administrator on a management network that is isolated from other switch traffic. You can also manage the switch module through any of the external uplink ports.

Table 1 describes the switch module ports. Each external port has an associated LED.

Table 1 Cisco Catalyst Blade Switch 3020 for HP Port Descriptions

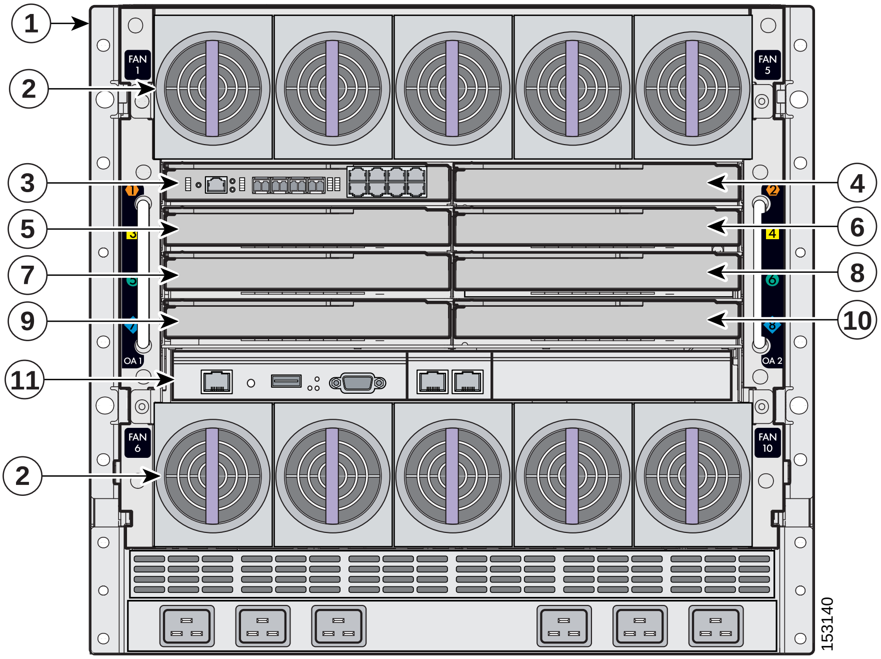
Port	Description
Ports 1 to 16	Internal Gigabit Ethernet 1000BASE-X downlink ports.
Ports 17 to 20 and Ports 17x to 20x	Dual-purpose SFP module/RJ-45 copper Ethernet uplink ports. The SFP module ports support only Cisco 1000BASE-SX fiber-optic modules. By default, the switch module dynamically selects the interface type that first links up. SFP modules have precedence if both SFP module and copper Ethernet interface types are in link-up state. You can also specifically configure each port for either copper Ethernet or SFP modules if you do not want to use autodetection. The copper Ethernet ports support automatic medium-dependent interface crossover (auto-MDIX) and autonegotiation. For information about configuring speed and duplex settings for a dual-purpose uplink port, see the switch module software configuration guide.
Ports 21x to 22x	External 10/100/1000BASE-T copper Gigabit Ethernet uplink ports that support auto-MDIX, and autonegotiation.
Ports 23x to 24x	Dual-purpose external/internal 10/100/1000BASE-T copper Gigabit Ethernet uplink ports. These ports can be configured for internal 1000BASE-X cross-connection with a corresponding switch module. When ports 23x and 24x are in external operation mode, they support auto-MDIX and autonegotiation. The default is external operation mode.
Internal 100BASE-T Ethernet port	This port (fa0) is used only for switch module management traffic, not for data traffic. It is connected to the Onboard Administrator through the blade server backplane connector.
Console port	RJ-45 switch module management port.

The switch module is powered from the blade server backplane, and temperature management is provided by the blade server. There is no fan on the switch module.

3 HP c-Class BladeSystem Architecture

Figure 2 shows the rear view of the blade server, in which you install the switch module.

Figure 2 Rear View of the Blade Server



1	Blade server rear view	**7**	Interconnect module bay 5
2	Blade server fans	**8**	Interconnect module bay 6
3	Interconnect bay 1 with switch module installed	**9**	Interconnect module bay 7
4	Interconnect module bay 2	**10**	Interconnect module bay 8
5	Interconnect module bay 3	**11**	Onboard Administrator module
6	Interconnect module bay 4		

Consider these prerequisites before installing your switch module:

- Fill any unoccupied interconnect bays or any unoccupied power module bays in the blade server with blanks.
- Identify the bays in which you will insert the switch modules. Plan to install the first switch module in bay 1, the second in bay 2, and so on up to bay 8, if possible. The bay in which you choose to install each switch module depends on whether mezzanine or Ethernet cards are installed in the blade server and how they are configured. See the blade server documentation for more information about installing and configuring the mezzanine or Ethernet cards.

  The interconnect module bays are physically interconnected in pairs through the blade server backplane. That is, each of these pairs—bays 1 and 2, bays 3 and 4, bays 5 and 6, and bays 7 and 8—are interconnected. If you install two switch modules in one of the paired bays, they are internally interconnected. You must configure the switch modules to logically enable the interconnect ports, Gigabit Ethernet ports 23 and 24. See the switch module software configuration guide for information on configuring these ports.
- See the HP c-Class documentation for information on the port mapping between blade servers and the switch modules.

4 Installing the Switch Module in the Blade Server

Before you install the switch module in the blade server, consider these points:

- Review and become familiar with the safety guidelines in the *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3020 for HP* that accompanies this guide.
- Review and become familiar with the safety guidelines in the HP BladeSystem enclosure setup and installation guide.
- Review and become familiar with the temperature, power, and grounding requirements specified in the HP BladeSystem enclosure setup and installation guide.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Caution To prevent electrostatic-discharge (ESD) damage when installing switch modules, follow your normal board and component handling procedures.

Note When you install a switch module, you do not need to power down the blade server.

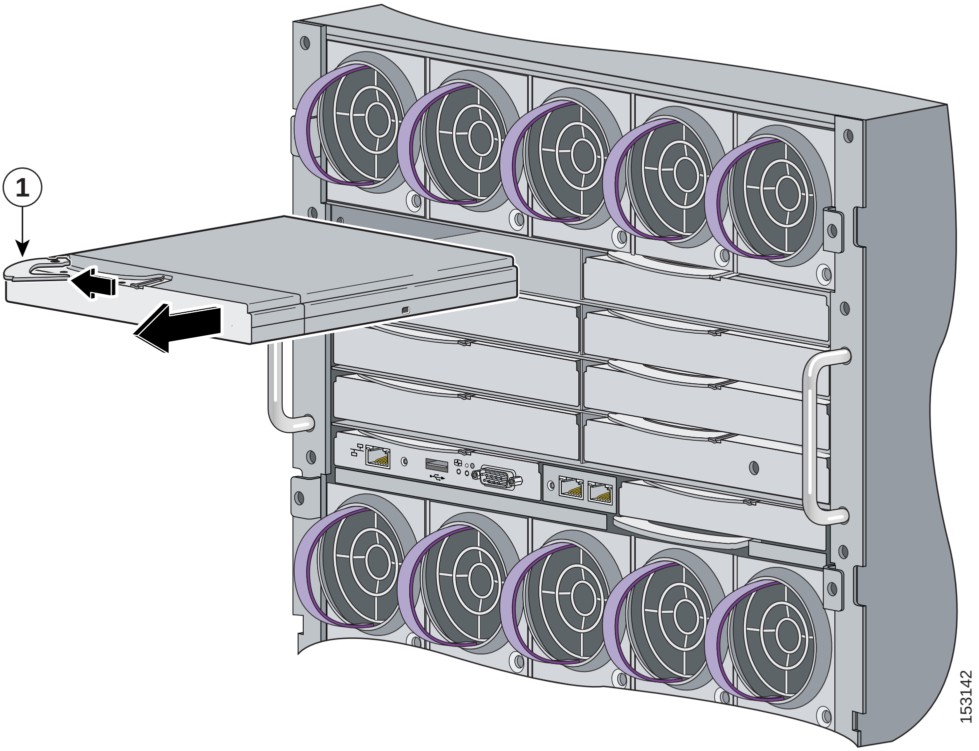
Follow these steps to install the switch module in the blade server:

Step 1 If you have not already done so, touch the static-protective package that contains the switch module to an unpainted metal part of the blade server for at least 2 seconds.

Step 2 Remove the switch module from its static-protective package.

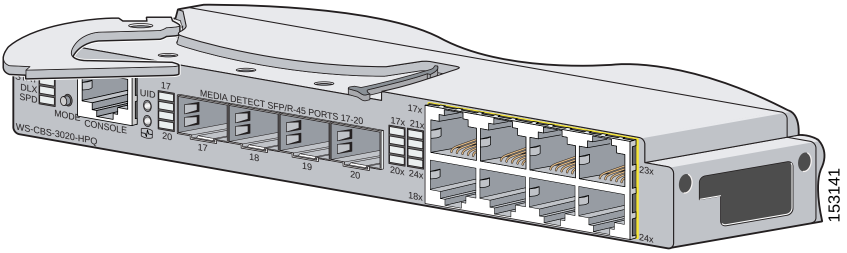
Step 3 Remove the interconnect blank from the bay where you plan to install the switch module, if one is present, and install the switch module. (See Figure 3.)

Figure 3 Removing the Interconnect Module Blank from the Blade Server



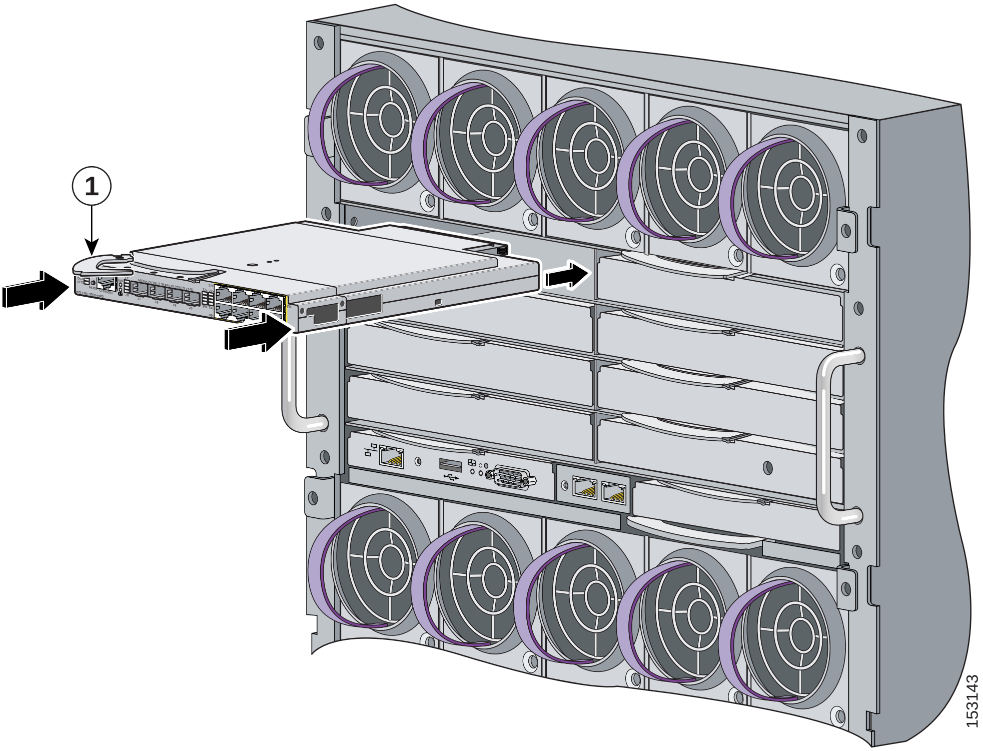
1	Lever for the interconnect module blank

Step 4 Ensure that the release latch on the switch module is in the open position (perpendicular to the module):



Step 5 Slide the switch module into the bay until it stops. (See Figure 4.)

Figure 4 Installing the Switch Module into the Blade Server Interconnect Module Bay



1	Switch module release latch

Step 6 Push the release latch on the front of the switch module to the closed position.

Switch Module IP Addresses

IP addresses can be assigned to two of the switch module interfaces:

- The fa0 Ethernet interface. This Layer 3 Ethernet interface is connected to the Onboard Administrator through which you can manage the switch module. It is used only for switch module management traffic, not for data traffic.
- The VLAN 1 interface. You can manage the switch module from any of its external ports through VLAN 1.

If you want to assign the VLAN 1 IP address through Express Setup, you must start that process immediately after installing the switch module in the blade server. If you miss the opportunity to have the IP address assigned in this way, you can remove and then re-install the switch module. See the "Running Express Setup" section on page 9 for instructions.

When you install the switch module, you need to determine whether the Onboard Administrator is connected to a network in which a DHCP server is also connected or if the Onboard Administrator has been configured as a DHCP server. If either of these conditions is true, the switch module automatically obtains an IP address for its fa0 Ethernet interface that is connected to the Onboard Administrator. In this case, a VLAN 1 IP address is not assigned, and to set up the switch module by using the Device Manager you must use the fa0 interface IP address that the DHCP server assigns.

See the "Using the Onboard Administrator to Assign an IP Address to the Switch Module fa0 Interface" section on page 14 for how to set up the switch module if the IP address is being assigned dynamically.

5 Running Express Setup

You need to supply this equipment to run Express Setup:

- PC
- Ethernet (Category 5) straight-through cable (as shown)

Before you run Express Setup, you must set up your switch module to communicate with a Hyperterminal program.

Note The initial configuration assumes that the switch module was never configured, that it is in the same state as when it was received, and that it is not configured with a default username and password.

Note To set up the switch module by using the command-line interface (CLI), see the switch module hardware installation guide on cisco.com.

Information You Need to Run Express Setup

You need this information about your switch module from your system administrator before you complete the setup program:

- Fixed IP address
- Subnet mask (IP netmask)
- Default gateway IP address

You can also configure these optional parameters through the Express Setup program:

- Local access password
- Telnet access password
- Names of the SNMP read and write community strings if you are going to use a network-management program like CiscoWorks.
- Host name, system contact, and system location

When you first set up the switch module, you can use Express Setup to enter the initial IP information. Doing this enables the switch module to connect to local routers and the Internet. You can then access the switch module through the IP address for further configuration.

Using Express Setup to Assign a VLAN 1 IP Address to the Switch Module

Use these steps to assign an IP address to the VLAN 1 interface through Express Setup. You must start these steps immediately after you have installed the switch module (see the "Installing the Switch Module in the Blade Server" section on page 6).

Note If approximately 2 minutes pass after you press the Mode button, obtaining the VLAN 1 IP address through Express Setup is no longer possible unless you remove and then re-install the switch module.

To prepare the switch module:

Step 1 Verify that no devices are connected to the switch module, because during Express Setup, the switch module acts as a DHCP server. If your PC has a static IP address, before you begin you should change your PC settings to temporarily use DHCP.

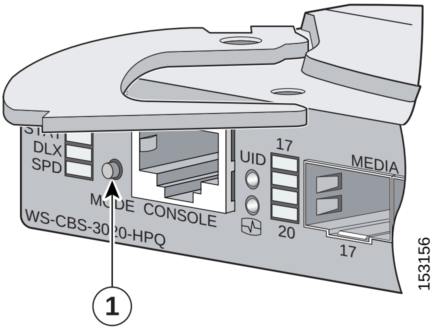
As the switch module powers on, it begins the power-on self-test (POST), a series of tests that runs automatically to ensure that the switch module functions properly.

Step 2 Wait for the switch module to complete POST. It might take several minutes for the switch module to complete POST.

Step 3 Verify that POST has completed by confirming that the system and status LEDs remain green.

If the switch module fails POST, the system LED turns amber. If the POST fails, see the "In Case of Difficulty" section on page 21 to determine a course of action. POST errors are usually fatal. Call Cisco Systems immediately if your switch module fails POST.

Step 4 Press and hold the Mode button until the four LEDs next to the Mode button turn green. This takes approximately 3 seconds.



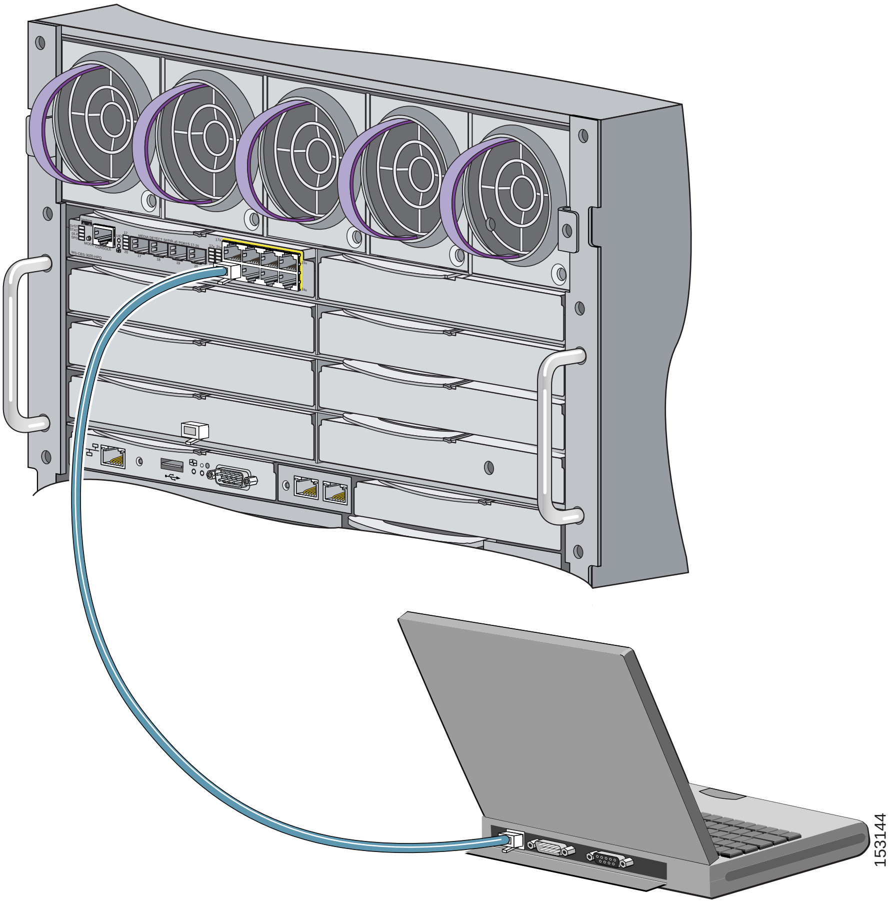
1	Mode button

Step 5 Release the Mode button.

If the LEDs next to the Mode button begin to blink after you press the button, release it. Blinking LEDs mean that the switch module has already been configured and cannot go into Express Setup mode. For more information, see the “Resetting the Switch Module” section on page 23.

Step 6 Connect a straight-through Category 5 Ethernet cable (not provided) to any Ethernet port on the switch module front panel and to the Ethernet port on the PC. (See Figure 5.)

Figure 5 Connecting the Ethernet Cable from a PC to a Switch Module Ethernet Port

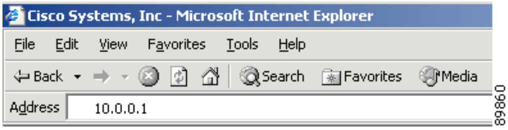


Caution Do not connect the switch module to any device other than the PC or workstation being used to configure it.

Step 7 Connect the other end of the cable to the Ethernet port on the PC or workstation. Verify that the port status LEDs on both connected Ethernet ports are green.

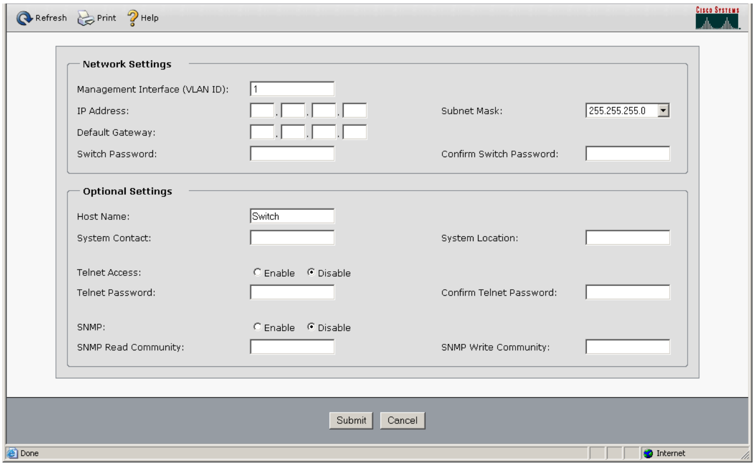
Step 8 Wait approximately 30 seconds *after* the port LEDs turn green, and launch a web browser on your PC or workstation.

Step 9 Enter the IP address 10.0.0.1 and press Enter.


Cisco Systems, Inc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
89860

Address 10.0.0.1

The Express Setup home page appears.



Network Settings

Management Interface (VLAN ID): 1

IP Address: . . .   Subnet Mask: 255.255.255.0

Default Gateway: . . .

Switch Password: Confirm Switch Password:

Optional Settings

Host Name: Switch

System Contact: System Location:

Telnet Access: ○ Enable ● Disable

Telnet Password: Confirm Telnet Password:

SNMP: ○ Enable ● Disable

SNMP Read Community: SNMP Write Community:

Step 10 Go to "Completing the Express Setup Fields" section on page 17 to finish setting up the switch module using the Express Setup screen of the Device Manager.

Using the Onboard Administrator to Assign an IP Address to the Switch Module fa0 Interface

For the switch module to obtain an IP address for the fa0 interface through the Onboard Administrator, these conditions must be met:

- The blade server is powered on and connected to the network.
- Basic configuration of the Onboard Administrator is completed, and you have the username and password for the Onboard Administrator.
- A DHCP server is configured on the network segment to which the blade server is connected, or the Onboard Administrator is configured to run as a DHCP server.

Note See the Onboard Administrator user guide at http://www.hp.com/go/bladesystem/documentation for more information about configuring and using the Onboard Administrator.

After you install the switch module in the interconnect module bay, after approximately 2 minutes, the switch module automatically obtains an IP address for its fa0 interface through the Onboard Administrator. This method of obtaining an IP address occurs if a DCHP server is configured on the same network, or if the Onboard Administrator is configured as a DHCP server. If you prefer to use Express Setup to assign the switch module IP address to the VLAN 1 interface, you must start the Express Setup steps immediately after you install the switch module.

After you have installed the switch module (see the "Installing the Switch Module in the Blade Server" section on page 6), it powers on. As it powers on, the switch module begins the POST, a series of tests that runs automatically to ensure that the switch module functions properly.

Step 1 Wait for the switch module to complete POST. It might take several minutes for the switch module to complete POST.

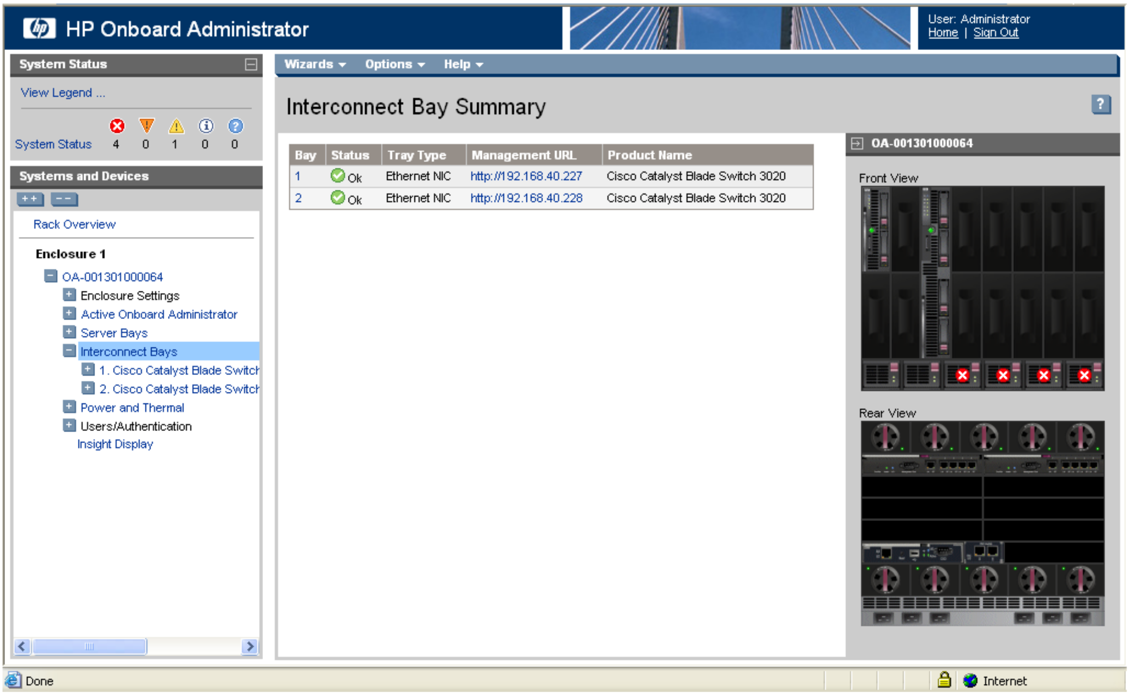
Step 2 Verify that POST has completed by confirming that the system and status LEDs remain green.

If the switch module fails POST, the system LED turns amber. If the POST fails, see the "In Case of Difficulty" section on page 21 to determine a course of action. POST errors are usually fatal. Call Cisco Systems immediately if your switch module fails POST.

Step 3 Wait approximately 2 minutes for the switch module to get the software image from its flash memory and begin autoinstallation.

Step 4 Using a PC that is connected to the same network segment as the blade server Onboard Administrator, access the Onboard Administrator in a browser window.

Step 5 Click Enclosure > Interconnect Bays to open the Interconnect Bay Summary window where you can find the assigned IP address of the switch module fa0 interface in the Management URL column.



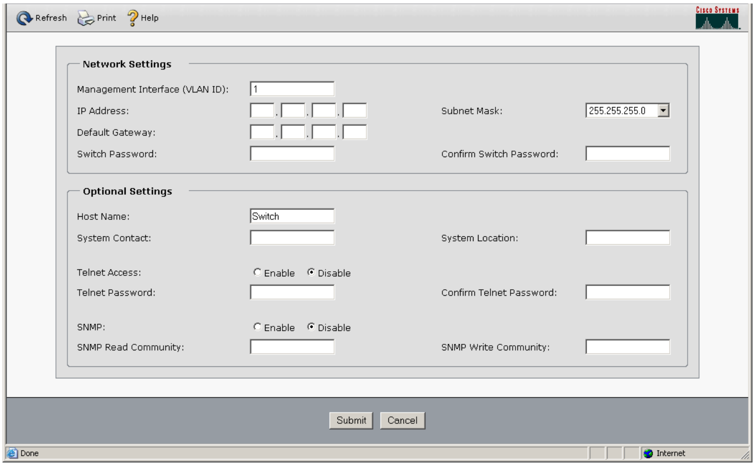
Bay	Status	Tray Type	Management URL	Product Name
1	Ok	Ethernet NIC	http://192.168.40.227	Cisco Catalyst Blade Switch 3020
2	Ok	Ethernet NIC	http://192.168.40.228	Cisco Catalyst Blade Switch 3020

153560

Step 6 Click the IP address hyperlink for the switch module from the Management URL column to open a new browser window. The Device Manager window for the switch module opens.

Step 7 On the left side of the Device Manager GUI, click Configuration > Express Setup.

The Express Setup page appears.



Network Settings

Management Interface (VLAN ID): 1

IP Address: . . .

Subnet Mask: 255.255.255.0

Default Gateway: . . .

Switch Password:

Confirm Switch Password:

Optional Settings

Host Name: Switch

System Contact:

System Location:

Telnet Access: ○ Enable ● Disable

Telnet Password:

Confirm Telnet Password:

SNMP: ○ Enable ● Disable

SNMP Read Community:

SNMP Write Community:

Step 8 Go to "Completing the Express Setup Fields" section on page 17 to finish setting up the switch module using the Express Setup screen of the Device Manager.

Completing the Express Setup Fields

Follow these steps to finish setting up the switch module:

Step 1 Enter this information in the Network Settings fields:

- In the Management Interface (VLAN ID) field, the default is 1. Enter a new VLAN ID only if you want to change the management interface through which you manage the switch module and to which you assign IP information. The VLAN ID range is 1 to 1001.
- In the IP Address field, enter the IP address of the switch module. In the IP Subnet Mask field, click the drop-down arrow, and select an IP Subnet Mask.
- In the Default Gateway field, enter the IP address for the default gateway (router).
- Enter your password in the Switch Password field. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the Confirm Switch Password field, enter your password again.

Step 2 (Optional) You can enter the Optional Settings information now or enter it later by using the device manager interface:

- In the Host Name field, enter a name for the switch module. The host name is limited to 31 characters; embedded spaces are not allowed.
- In the System Contact field, enter the name of the person who is responsible for the switch module. In the System Location field, enter the wiring closet, floor, or building where the switch module is located.
- In the Telnet Access field, click Enable if you are going to use Telnet to manage the switch module by using the CLI. If you enable Telnet access, you must enter a Telnet password.
- In the Telnet Password field, enter a password. The Telnet password can be from 1 to 25 alphanumeric characters, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the Confirm Telnet Password field, re-enter the Telnet password.
- In the SNMP field, click Enable to enable Simple Network Management Protocol (SNMP). Enable SNMP only if you plan to manage switches by using CiscoWorks 2000 or another SNMP-based network-management system.

  If you enable SNMP, you must enter a community string in the SNMP Read Community field, the SNMP Write Community field, or both. SNMP community strings authenticate access to MIB objects. Embedded spaces are not allowed in SNMP community strings. When you set the SNMP read community, you can access SNMP information, but you cannot modify it. When you set the SNMP write community, you can both access and modify SNMP information.

Step 3 Click Submit to save your settings, or click Cancel to clear your settings.

When you click Submit, the switch module is configured and exits Express Setup mode. The PC displays a warning message and then attempts to connect with the new switch module IP address. If you configured the switch module with an IP address that is in a different subnet from the PC, connectivity between the PC and the switch module is lost.

Step 4 Disconnect the switch module from the PC, and install the switch module in your network. See the “Managing the Switch Module” section on page 19 for information about configuring and managing the switch module.

If you need to rerun Express Setup, see the “Resetting the Switch Module” section on page 23.

To install additional switch modules, repeat the steps in the “Installing the Switch Module in the Blade Server” section on page 6 through the “Running Express Setup” section on page 9.

Refreshing the PC IP Address

After you complete Express Setup, you should refresh the PC IP address:

- For a dynamically assigned IP address, disconnect the PC from the switch module, and reconnect the PC to the network. The network DHCP server assigns a new IP address to the PC.
- For a statically assigned IP address, change it to the previously configured IP address.

6 Managing the Switch Module

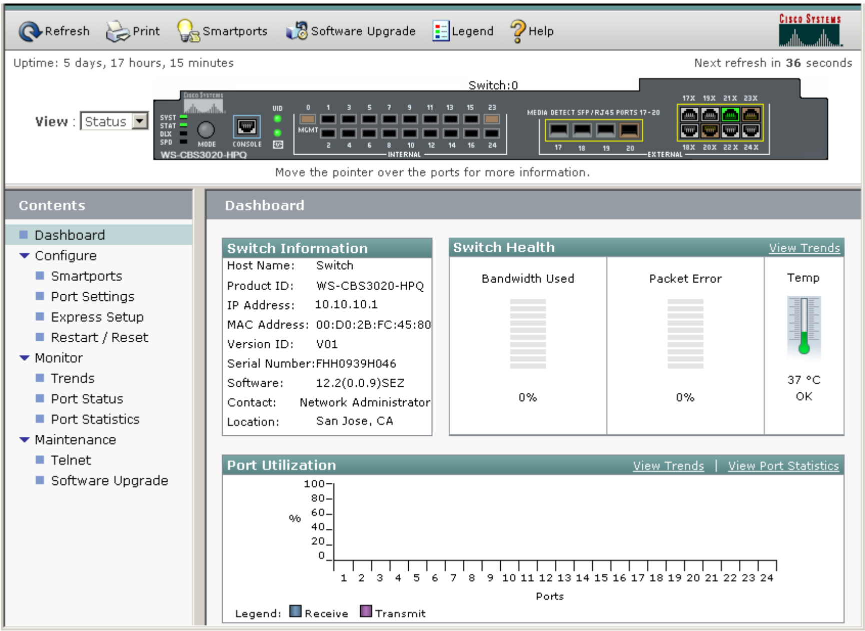
After you complete Express Setup and install the switch module in your network, use the device manager or other management options described in this section for further configuration.

Using the Device Manager

The simplest way to manage the switch module is by using the device manager that is in the switch module memory. This is a web interface that offers quick configuration and monitoring. You can access the device manager from anywhere in your network through a web browser.

Follow these steps:

1. Launch a web browser on your PC or workstation.
2. Enter the switch module IP address in the web browser, and press Enter. The device manager page appears.



Uptime: 5 days, 17 hours, 15 minutes

Next refresh in **36** seconds

Move the pointer over the ports for more information.

Dashboard

Switch Information

Host Name: Switch
Product ID: WS-CBS3020-HPQ
IP Address: 10.10.10.1
MAC Address: 00:D0:2B:FC:45:80
Version ID: V01
Serial Number: FHH0939H046
Software: 12.2(0.0.9)SEZ
Contact: Network Administrator
Location: San Jose, CA

Switch Health

Bandwidth Used	Packet Error	Temp
0%	0%	37 °C OK

Port Utilization

3. Use the device manager to perform basic switch module configuration and monitoring. Refer to the device manager online help for more information.
4. For more advanced configuration, download and run the Cisco Network Assistant, which is described in the next section.

Command-Line Interface

You can enter Cisco IOS commands and parameters through the CLI. Access the CLI either by connecting your PC directly to the switch module console port or through a Telnet session from a remote PC or workstation.

Follow these steps:

1. Connect the supplied RJ-45-to DB-9 adapter cable to the standard 9-pin serial port on the PC. Connect the other end of the cable to the console port on the switch module.
2. Start a terminal-emulation program on the PC.
3. Configure the PC terminal emulation software for:
   - 9600 baud
   - 8 data bits

   - No parity
   - 1 stop bit
   - No flow control
4. Use the CLI to enter commands to configure the switch module. See the software configuration guide and the command reference for more information.

Other Management Options

You can use SNMP management applications such as CiscoWorks Small Network Management Solution (SNMS) to configure and manage the switch module. You also can manage it from an SNMP-compatible workstation that is running platforms such as HP OpenView or SunNet Manager.

The Cisco IE2100 Series Configuration Registrar is a network management device that works with embedded Cisco Networking Services (CNS) agents in the switch module software. You can use IE2100 to automate initial configurations and configuration updates on the switch module.

See the “Accessing Help Online” section on page 23 for a list of supporting documentation.

Onboard Administrator Command-Line Interface

See the HP BladeSystem enclosure setup and installation guide at http://www.hp.com/go/bladesystem/documentation for information on how to use the Onboard Administration CLI.

7 In Case of Difficulty

If you experience difficulty, help is available in this section and also on Cisco.com. This section includes Express Setup troubleshooting, how to reset the switch module, how to access online help, and where to find more information.

Troubleshooting Express Setup

If Express Setup does not run, or if the Express Setup page does not appear in your browser:

- Did you verify that POST successfully ran before starting Express Setup?

  If not, make sure that only the SYST and STAT LEDs are green before pressing the Mode button to enter the Express Setup mode.

- Did you press the Mode button while the switch module was still running POST?

  If yes, wait until POST completes. Power cycle the switch module. Wait until POST completes. Confirm that the SYST and STAT LEDs are green. Press the Mode button to enter Express Setup mode.

- Did the switch module not power up?

  The switch module is controlled by the Onboard Administrator. If the switch module does not power up, see the blade server documentation for more information.

- Did you try to continue without confirming that the switch module was in Express Setup mode?

  Verify that all LEDs next to the Mode button are green. If necessary, press the Mode button to enter Express Setup mode.

- Does your PC have a static IP address?

  If yes, before connecting to the switch module, change your PC settings to temporarily use DHCP.

- Did you connect a crossover cable instead of a straight-through Ethernet cable between a switch module port and the Ethernet port of the PC?

  If yes, connect a straight-through cable to an Ethernet port on the switch module and the PC. Wait 30 seconds before you enter 10.0.0.1 in the browser.

- Did you connect the Ethernet cable to the console port instead of to an Ethernet port on the switch module?

  If yes, disconnect the cable from the console port. Then connect the cable to an Ethernet port on the switch module and the PC. Wait 30 seconds before you enter 10.0.0.1 in the browser.

• Did you wait 30 seconds after you connected the switch and the PC before you entered the IP address in your browser?	If not, wait 30 seconds, re-enter 10.0.0.1 in the browser, and press Enter.
• Did you enter the wrong address in the browser, or is there an error message?	If yes, re-enter 10.0.0.1 in the browser, and press Enter.

Resetting the Switch Module

This section describes how to reset the switch module by rerunning Express Setup. These are reasons why you might want to reset the switch module:

- You installed the switch module in your network and cannot connect to it because you assigned the incorrect IP address.
- You want to clear all configurations from the switch module and assign a new IP address.
- You are trying to enter Express Setup mode, and the switch module LEDs start blinking when you press the Mode button (which means that the switch module is already configured with IP information).

Caution Resetting the switch module deletes the configuration and reboots the switch module.

To reset the switch module, press and hold the Mode button. The switch module LEDs begin blinking after about 3 seconds. Continue holding down the Mode button. The LEDs stop blinking after 7 more seconds, and then the switch module reboots.

The switch module now behaves like an unconfigured switch module. You can enter the switch module IP information by using Express Setup as described in the "Running Express Setup" section on page 9.

Accessing Help Online

First look for a solution to your problem in the troubleshooting section of the *Cisco Catalyst Blade Switch 3020 for HP Hardware Installation Guide* or the *Cisco Catalyst Blade Switch 3020 for HP Software Configuration Guide* on Cisco.com. You can also access the Cisco Technical Support and Documentation website for a list of known hardware problems and extensive troubleshooting documentation, including:

- Factory defaults and password recovery
- Recovery from corrupted or missing software
- Switch module port problems

- Network interface cards
- Troubleshooting tools
- Field notices and security advisories

Follow these steps:

1. Open your browser, and go to http://www.cisco.com/.
2. Click Technical Support and Documentation.
3. Click Tools and Resources.
4. Under Jump to, click **Troubleshooting**.
5. Click the subject that addresses the problem that you are experiencing.

For More Information

For more information about the switch module, see these documents on Cisco.com:

- *Cisco Catalyst Blade Switch 3020 for HP Hardware Installation Guide* (not orderable, but available on Cisco.com). This guide provides complete hardware descriptions and detailed installation procedures.
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3020 for HP* (order number DOC-7817607=). This guide contains agency approvals, compliance information, and translated warning statements.
- *Release Notes for the Cisco Catalyst Blade Switch 3020 for HP* (not orderable but available on Cisco.com)
- *Cisco Catalyst Blade Switch 3020 for HP Software Configuration Guide* (not orderable, but available on Cisco.com). This guide provides a product overview and detailed descriptions and procedures for the switch module software features.
- *Cisco Catalyst Blade Switch 3020 for HP Command Reference* (not orderable, but available on Cisco.com). This reference provides detailed descriptions of the Cisco IOS commands specifically created or modified for the switch module.
- *Cisco Catalyst Blade Switch 3020 for HP System Message Guide* (not orderable, but available on Cisco.com). This guide provides descriptions of the system messages specifically created or modified for the switch module.

8 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

9 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

10 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

11 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

12 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

13 Hardware Warranty Terms

These sections describe the warranty terms for the switch:

- If you purchased the Cisco Catalyst Blade Switch 3020 for HP from Cisco, see the "Cisco 90-Day Limited Hardware Warranty Terms" section on page 31.
- If you purchased the Cisco Catalyst Blade Switch 3020 for HP from HP or an HP Authorized Reseller, see the "HP Hardware Warranty Terms" section on page 32 for specific HP warranty information.

Cisco 90-Day Limited Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranties and license agreements applicable to Cisco software, is available on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty and license agreements from Cisco.com.

1. Launch your browser, and go to this URL:

   http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

   The Warranties and License Agreements page appears.

2. To read the *Cisco Information Packet*, follow these steps:

   a. Click the Information Packet Number field, and make sure that the part number 78-5235-03B0 is highlighted.

   b. Select the language in which you would like to read the document.

   c. Click Go.

   The Cisco Limited Warranty and Software License page from the Information Packet appears.

   d. Read the document online, or click the PDF icon to download and print the document in Adobe Portable Document Format (PDF).

   Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website: http://www.adobe.com

3. To read translated and localized warranty information about your product, follow these steps:

   a. Enter this part number in the Warranty Document Number field:

   78-5236-01C0

   b. Select the language in which you would like to read the document.

c. Click Go.

The Cisco warranty page appears.

d. Review the document online, or click the PDF icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

http://www.cisco.com/public/Support_root.shtml.

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of a Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference:

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	

HP Hardware Warranty Terms

This section provides the limited warranty and material limitations for the HP ProLiant and X86 Servers and Options.

Limited Warranty and Material Limitations

Each product is sold subject to the express limited warranty statement relating to that product. THE GLOBAL LIMITED WARRANTY AND TECHNICAL SUPPORT STATEMENT PROVIDES IMPORTANT INFORMATION ABOUT THE NATURE AND SCOPE OF THE EXPRESS LIMITED

WARRANTY PROVIDED FOR THE HP PRODUCT, AND ALSO CONTAINS CERTAIN DISCLAIMERS AND LIMITATIONS OF LIABILITY BY HP, WHICH MATERIALLY IMPACT YOUR RIGHTS. ACCORDINGLY, YOU ARE STRONGLY ADVISED TO CAREFULLY READ THE GLOBAL LIMITED WARRANTY AND TECHNICAL SUPPORT STATEMENT BEFORE USING YOUR HP PRODUCT. YOUR USE OF THE HP PRODUCT IS DEEMED TO BE ACCEPTANCE OF THE TERMS AND CONDITIONS SET FORTH IN THE GLOBAL LIMITED WARRANTY AND TECHNICAL SUPPORT STATEMENT.

You can view, print, or download the global limited warranty and technical support statement for ProLiant and X86 servers and options at

http://h18004.www1.hp.com/products/servers/platforms/warranty/index.html

If you do not have access to the website, you can use this form to order a printed copy of the global limited warranty and technical support statement.

Document:
Global Limited Warranty and Technical Support - HP ProLiant and X86 Servers and Options

Step 1. Enter product information (REQUIRED):
Date of Purchase:

Step 2. Enter delivery address:		
Company Name:		
Name:		
Address: (No P.O. Boxes)		
City:	State/Province:	Zip/Postal Code
Country:		Phone Number:
Email:		

Step 3. Place your order:	
Fax this form to 1-800-469-1690 (toll-free in U.S. and Canada	Fax this form to 1-281-518-1599 (toll outside U.S. and Canada)

保証規定について

この製品にはHPの製品保証が適用されます。製品に不具合があった場合には、HPおよびHP正規保守代理店が保証規定に基づく保証サービスを提供いたします。保証規定書および保証書は、製品に添付されている場合と製品に添付されていない場合があります。保証規定書が添付されていない場合にはWebサイト（www.hp.com/jp/support/warranty_server）に掲載されている保証規定をご覧ください。

保証期間は製品お買い上げ日から開始します。お客様が保証サービスをご利用になる場合には、製品のお買い上げ日が証明される書類（領収書、納品書など）をご提示いただくことが必要となります。保証書が添付されている製品では、所定事項が記入され、販売店印のある保証書が製品のお買い上げ日を証明します。

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

♲ Printed in the USA on recycled paper containing 10% postconsumer waste.

78-17364-02
DOC-7817364=